

Chapter 10

Intrusion Detection Services Configuration Guidelines

The Adaptive Services Physical Interface Card (AS PIC) supports a limited set of intrusion detection services (IDS) to perform attack detection. You can use IDS to perform the following tasks:

- Detect various types of denial-of-service (DoS) and directed denial-of-service (DDoS) attacks.

- Detect attempts at network scanning and probing.

- Detect anomalies in traffic patterns, such as sudden bursts or a decline in bandwidth.

- Prevent some types of attacks.

- Redirect attack traffic to a collector for analysis.

The IDS configuration allows you to focus the attack detection and remedial actions on specific hosts or networks that you specify in the IDS terms. Signature detection is not supported.

To configure intrusion detection services, you include the following statements at the [edit services] hierarchy level of the configuration:

```
[edit services]
ids {
  rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
      from {
        applications [ application-names ];
        application-sets [ set-names ];
        destination-address address;
        source-address address;
      }
      then {
        aggregation {
          destination-prefix prefix-value;
          source-prefix prefix-value;
        }
        (force-entry | ignore-entry);
        logging {
          syslog;
          threshold rate;
        }
        syn-cookie {
          mss value;
          threshold rate;
        }
      }
    }
  }
  rule-set rule-set-name {
    [ rule rule-names ];
  }
}
```



NOTE: The JUNOS software uses stateful firewall settings as a basis for performing IDS. You must commit a stateful firewall configuration in the same service set for IDS to function properly.

This chapter describes the following tasks for configuring intrusion detection services:

Configuring Intrusion Detection Properties on page 95

Examples: Configuring Intrusion Detection Properties on page 100

Configuring Intrusion Detection Properties

This section describes the following tasks for configuring intrusion detection services:

Configuring the IDS Rule Set on page 95

Configuring IDS Rule Content on page 95

Configuring the IDS Rule Set

The rule-set statement defines a collection of IDS rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the rule-set statement at the [edit services ids] hierarchy level:

```
[edit services ids]
rule-set rule-set-name {
  rule rule-name1;
  rule rule-name2;
  rule rule-name3;
  ...
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, the packet is dropped by default.

Configuring IDS Rule Content

IDS rules identify traffic for which you want the router software to count events. Because IDS is based on stateful firewall properties, you must configure at least one stateful firewall rule and include it in the service set with the IDS rules; for more information, see “Stateful Firewall Services Configuration Guidelines” on page 63.

To configure an IDS rule, include the rule *rule-name* statement at the [edit services ids] hierarchy level:

```
[edit services ids]
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      applications [ application-names ];
      application-sets [ set-names ];
      destination-address address;
      source-address address;
    }
    then {
      aggregation {
        destination-prefix prefix-value;
        source-prefix prefix-value;
      }
      (force-entry | ignore-entry);
      logging {
        syslog;
        threshold rate;
      }
      syn-cookie {
        mss value;
        threshold rate;
      }
    }
  }
}
```

Each IDS rule consists of a set of terms, similar to a filter configured at the [edit firewall] hierarchy level. A term consists of the following:

from statement—Specifies the match conditions and applications that are included and excluded.

then statement—Specifies the actions and action modifiers to be performed by the router software.

In addition, each rule includes a match-direction statement that specifies whether the match is applied on the input or output side of the interface. To configure where the match is applied, include the match-direction (input | output) statement at the [edit services ids rule *rule-name*] hierarchy level:

```
[edit services ids]
rule rule-name {
  match-direction (input | output | input-output);
}
```

If you configure match-direction input-output, bidirectional rule creation is allowed.

The following sections describe IDS rule content in more detail:

Configuring IDS Match Conditions on page 97

Configuring IDS Actions on page 98

Configuring IDS Match Conditions

To configure IDS match conditions, include the from statement at the [edit services ids rule *rule-name* term *term-name*] hierarchy level:

```
[edit services ids rule rule-name term term-name]
from {
  applications [ application-names ];
  application-sets [ set-names ];
  destination-address address;
  source-address address;
}
```

If you omit the from statement, the software accepts all events and places them in the IDS cache for processing.

You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the *JUNOS Policy Framework Configuration Guide*.

You can also include application protocol definitions that you have configured at the [edit applications] hierarchy level; for more information, see “Applications Configuration Guidelines” on page 43:

To apply one or more specific application protocol definitions, include the applications statement at the [edit services ids rule *rule-name* term *term-name* from] hierarchy level.

To apply one or more sets of application protocol definitions that you have defined, include the application-sets statement at the [edit services ids rule *rule-name* term *term-name* from] hierarchy level.



NOTE: If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the [edit applications] hierarchy level; you cannot specify these properties as match conditions.

If a match occurs on an application, the application protocol is displayed separately in the show command output. For more information, see the *JUNOS Network and Services Interfaces Command Reference*.

Configuring IDS Actions

To configure IDS actions, include the then statement at the [edit services ids rule *rule-name* term *term-name*] hierarchy level:

```
[edit services ids rule rule-name term term-name]
then {
  aggregation {
    destination-prefix prefix-value;
    source-prefix prefix-value;
  }
  (force-entry | ignore-entry);
  logging {
    syslog;
    threshold rate;
  }
  syn-cookie {
    mss value;
    threshold rate;
  }
}
```

You can configure the following possible actions:

aggregation—The router aggregates traffic labeled with the specified source or destination prefixes before passing the events to IDS processing. This is helpful if you want to examine all the traffic connected with a particular source or destination host. To collect traffic with some other marker, such as a particular application or port, configure that value in the match conditions.

To configure, include the aggregation statement at the [edit services ids rule *rule-name* term *term-name* then] hierarchy level and specify values for source-prefix or destination-prefix:

```
[edit services ids rule rule-name term term-name then]
aggregation {
  destination-prefix prefix-value;
  source-prefix prefix-value;
}
```

The range for the source-prefix and destination-prefix statements is restricted to integers from 1 through 32.

force-entry—The entry is assured a permanent spot in IDS caches after one event is registered. By default, the IDS software does not record information about “good” packets that do not exhibit suspicious behavior. You can use the force-entry statement to record all traffic from a suspect host, even traffic that would not otherwise be counted.

ignore-entry ensures that all IDS events are ignored. You can use this statement to disregard all traffic from a host you trust, including any temporary anomalies that IDS would otherwise count as events.

To configure, include the `force-entry` or `ignore-entry` statement at the [edit services ids rule *rule-name* term *term-name* then] hierarchy level:

```
[edit services ids rule rule-name term term-name then]
(force-entry | ignore-entry);
```

`logging`—The event is logged in the system log file.

To configure, include the `logging` statement at the [edit services ids rule *rule-name* term *term-name* then] hierarchy level:

```
[edit services ids rule rule-name term term-name then]
logging {
  syslog;
  threshold rate;
}
```

You can optionally include a threshold rate to trigger logging activity or activate the generation of system log messages. The threshold rate is specified in events per second.

`syn-cookie`—The router activates syn-cookie defensive mechanisms.

To configure, include the `syn-cookie` statement at the [edit services ids rule *rule-name* term *term-name* then] hierarchy level:

```
[edit services ids rule rule-name term term-name then]
syn-cookie {
  mss value;
  threshold rate;
}
```

If you enable syn-cookie defenses, you must include both a threshold rate to trigger syn-cookie activity and a TCP maximum sequence selection (MSS) value for TCP delayed binding. The threshold rate is specified in SYN attacks per second. By default, the TCP MSS value is 1500; the range is from 128 through 8192.

Examples: Configuring Intrusion Detection Properties

The following configuration adds a permanent entry to the IDS anomaly table when it encounters a flow with the destination address 104.410.6.2:

```
[edit services ids]
rule simple_ids {
  term 1 {
    from {
      destination-address 104.410.6.2/32;
    }
    then {
      force-entry;
      logging {
        threshold 1;
        syslog;
      }
    }
  }
  term default {
    then {
      aggregation {
        source-prefix 24;
      }
    }
  }
}
match-direction input;
```

The IDS configuration works in conjunction with the stateful firewall mechanism and relies heavily on the anomalies reported by the stateful firewall. The following configuration example shows this relationship:

```
[edit services ids]
rule simple_ids {
  term 1 {
    from {
      source-address 101.30.20.2/32;
      destination-address {
        101.30.10.2/32;
        101.30.1.2/32 except;
      }
      applications appl-ftp;
    }
    then {
      force-entry;
      logging {
        threshold 5;
        syslog;
      }
      syn-cookie {
        threshold 10;
      }
    }
  }
}
match-direction input;
```